サイドチャネル攻撃に対する認証暗号ソフトウェアの安全性評価に関する研究

修士学位論文要約（平成30年３月）

サイドチャネル攻撃に対する認証暗号ソフトウェアの安全性評価に関する研究

忍田 大和
指導教員：青木 孝文

Security Evaluation on Authenticated Encryption Software against Side-Channel Attacks

Hirokazu OSHIDA
Supervisor: Takafumi AOKI

This paper clarify a threat of side-channel attack against authenticated encryptions implemented on software. In particular, we focus on a major authenticated encryptions named AES-GCM, which is currently used in many applications. First, this paper presents an advanced power analysis attack that can be effective for AES-GCM software even with a masking countermeasure. The novel idea of the attack is to target authentication tag generation based on Galois field multiplication.

1. はじめに

ネットワークシステムへの攻撃方法の多様化に伴い，メッセージの機密性と完全性を同時に実現する認証暗号の需要が高まっている．現在，認証暗号としては国際標準暗号 AES (Advanced Encryption Standard) とガロア体上の演算に基づく改ざん検知を組み合わせた AES-GCM (Galois Counter Mode) が広く用いられている．また，近年では IoT (Internet of Things) と言われるようにありとあらゆるモノがインターネットに接続されるようになってきている．末端の機器においても通信の安全性を保証する必要から認証暗号がソフトウェアとして組み込まれる機会が増大すると考えられる．一方で，暗号処理を実装した機器への接触が容易になることで，暗号アルゴリズムが安全性を保証し得ない物理的な攻撃により暗号や改ざんの検知機構が破られる危険がある．特に，機器の動作中の消費電力や漏洩電磁波などを利用し，内部の秘密情報を奪うサイドチャネル攻撃は，攻撃の痕跡が残らないことなどから，暗号機器に対する現実的な脅威とされている．近年，AES-GCM の改ざん検知機構を破りうる強力な攻撃手法 [1] が提案された．しかし，同攻撃に対する対策法については論文中で述べられていないだけでなく，既存のサイドチャネル攻撃への汎用的な対策法が同攻撃に対して有効かどうかも分かっておらず，対策法の検討及びその安全性の評価が課題となっている．

本論文では，認証暗号 AES-GCM のサイドチャネル攻撃耐性評価を行う．具体的には，サイドチャネル攻撃への汎用的な既存対策であるマスキングを AES-GCM に適用し，マスキングが攻撃 [1] に対し有効であることを示す．その上で，同攻撃をマスキング対策に適用できるように拡張した新たな攻撃手法を提案し，実機を用いた実験を通してその実現可能性を計算量的に評価する．

2. AES-GCM へのサイドチャネル攻撃

AES-GCM を含む認証暗号では，送受信者が共有する鍵と呼ばれる秘密情報を用いて送受信の間のメッセージの改ざんを検知する．ここで，攻撃者が鍵を知った場合，攻撃者は任意のメッセージを受信者に改ざんがなかったものとして受け取らせることができる．すなわち，認証暗号の改ざん検知機構は鍵の秘密性に基づく．

攻撃 [1] は，AES-GCM の動作中の消費電力を測定することで，改ざん検知のための秘密情報である鍵を求める．同攻撃では，まず，AES-GCM 暗号モジュールに対して複数の既知情報を入力し，そのときの消費電力を計測する．そして，測定した消費電力をもとに，AES-GCM の出力とはならず内部で秘密裏に処理される演算結果の値を推定する．ここで，機器の消費電力は機器が処理しているデータに依存することを利用する．次に，入力した既知情報と推定した演算結果から，鍵についての方程式を多数立式する．演算結果は，入力した既知情報と鍵から計算される値であるため，演算結果と既知情報から鍵についての方程式を立式できる．最後に，立式した方程式を解くことで鍵を求める．

表 1　提案攻撃の時間計算量

SNR	Num. of traces: 2^{18}			Num. of traces: 2^{22}			Num. of traces: 2^{24}		
	Mem. 2^{25}	Mem. 2^{33}	Mem. 2^{46}	Mem. 2^{25}	Mem. 2^{33}	Mem. 2^{46}	Mem. 2^{25}	Mem. 2^{33}	Mem. 2^{46}
8	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	86.0
32	N/A	N/A	N/A	N/A	N/A	81.3	N/A	N/A	74.7
64	48.2	48.0	48.0	47.6	47.6	47.6	44.4	44.4	44.4

3.　サイドチャネル攻撃への既存対策

従来のサイドチャネル攻撃への汎用的な対策であるマスキングは，機器内部で処理される値を乱数により変換したうえで処理を行っていく．そのため，観測される消費電力は乱数の施された演算結果に依存し，真の演算結果とは独立となるため，消費電力から真の演算結果を推定することができなくなる．本論文では，マスキング対策が施された 8 ビット乗算に対して攻撃 [1] を適用した結果，攻撃が不可能となることを確認した．

4.　マスキングへの攻撃

マスキングでは，最終的な値を出力する直前で，施した乱数の影響を除去する必要があるが，そのための値であるアンマスク値を並列して計算することが一般的である．提案攻撃では，マスクされた演算結果およびアンマスク値のそれぞれを機器が処理する際の消費電力を計測し，それらから真の演算結果を推定することで，マスキングが施されている場合であっても鍵を取得できる．提案攻撃の可否は，立式した方程式を求解する際に利用可能なメモリ，SN 比（消費電力から演算結果がどれくらい正確に推定できるか），および波形数（入力できる既知乗数の個数）により左右される．表 1 に，提案攻撃の時間計算量を示す．ここで，”Mem.”は利用可能なメモリを表し，”N/A”は攻撃が不可能であることを意味する．SN 比が小さい場合と，計測波形数が小さい場合では攻撃が不可能になることが分かる．表 1 より，SN 比が大きい場合　(64∼) では提案攻撃が現実的な時間で実行可能であることが分かる．

5.　実験的評価

検証のため，8 ビットマイコンを搭載したスマートカード上に実装された AES-GCM に対して，評価実験を行った．実験環境を図 1 に示す．実験環境は，サイドチャネル攻撃評価用ボード (SASEBO-W: side-channel attack standard evaluation board) [2]，IC カード及びカード上の 8 ビットマイコン，力測定用のデジタルオシロスコープにより構成されている．処理中の消費電力から SN 比を算出したところ，107.9 を得た．上述の計算量的評価と合わせ，このことは提案攻撃の実現可能性を示している．

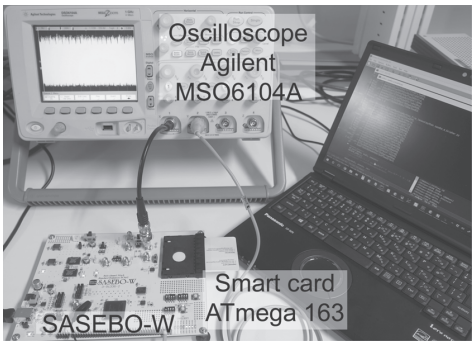

図 1　電力波形測定の実験環境

6.　まとめ

本論文では，AES-GCM ソフトウェアのサイドチャネル攻撃に対する安全性評価を行った．特に，同攻撃への既存対策であるマスキングに着目し，同対策の有効性を確認した．その上で，対策を無効化しうる新たな攻撃手法を提案し，その実現可能性を示した．

文献

1) Sonia Belaïd, Jean-Sb́astueb Coron, Pierre-Alain Fouque, Benoit Gérard, Jean-Gabriel Kammerer, and Emmanuel Prouff, “Improved side-channel analysis of finite-field multiplication,” in *Cryptographic Hardware and Embedded Systems (CHES)*, vol. 6917 of *Lecture Notes in Computer Scienece*, pp. 395–415, 2015.
2) “Side-channel attack standard evaluation board (sasebo).” `http://www.rcis.aist.go.jp/special/SASEBO`.